ОЦЕНКА ПОКАЗАТЕЛЕЙ КИБЕРУСТОЙЧИВОСТИ СИСТЕМ СБОРА И ОБРАБОТКИ ИНФОРМАЦИИ В ЭЭС НА ОСНОВЕ ПОЛУМАРКОВСКИХ МОДЕЛЕЙ[1]

Колосок И.Н.[2], Гурина Л.А.[3]

Цель исследования: *разработка алгоритма определения показателей киберустойчивости систем сбора, передачи и обработки информации для управления электроэнергетической системой (ЭЭС) — SCADA, WAMS, позволяющего учитывать возможные состояния и меры по восстановлению таких систем при нарушениях киберустойчивости.*

Методы исследования: *теория вероятностей, методы анализа надежности ЭЭС, марковские методы.*

Результат исследования: *проведен анализ надежности WAMS, необходимый для оценки киберустойчивости ЭЭС. Предложена модель киберустойчивости, на основе которой разработан алгоритм определения показателей киберустойчивости систем SCADA, WAMS при низком качестве измерительной информации, используемой при управлении ЭЭС. Для учета возможных состояний систем SCADA, WAMS и мер по их восстановлению (обнаружение, смягчение последствий и реагирование) при нарушении киберустойчиовсти в алгоритме используются инструментарий теории вероятностей и марковские методы. Эффективность применения разработанного алгоритма подтверждается на примере расчета показателя киберустойчивости WAMS при низком качестве синхронизированных векторных измерений. Полученные результаты могут быть полезны при принятии решений по формированию управляющих воздействий на ЭЭС для обеспечения ее кибербезопасности в условиях кибератак на системы сбора, обработки и передачи информации.*

Ключевые слова: *электроэнергетическая система, надежность, устойчивость, SCADA, WAMS, кибератаки, качество измерений, оценивание состояния.*

DOI:10.21681/2311-3456-2021-6-2-11

Введение

Киберфизические электроэнергетические системы (ЭЭС) [1] имеют сложную многоуровневую инфраструктуру, составляющими которой являются информационно-коммуникационная и физическая подсистемы. Эти подсистемы взаимосвязаны и взаимозависимы [2], подвержены изменениям в их среде, вызванными внутренними и внешними воздействиями, рост которых обусловлен увеличением уязвимостей из-за широкомасштабного внедрения информационных и вычислительных технологий, цифровизации систем энергетики [3]. Отказ компонентов одной подсистемы может привести к нарушению работы другой и, в конечном счете, к потере работоспособности всей ЭЭС [4-6]. При принятии решений по формированию управляющих воздействий в ЭЭС вопросы обеспечения киберустойчивости систем сбора, передачи и обработки информации для надежного функционирования ЭЭС [7, 8] становятся актуальным.

Киберустойчивость (Cyber resilience) ЭЭС основана на ее способности своевременно распознавать, приспосабливаться и устранять нарушения в информационно-коммуникационной подсистеме. Киберустойчивость подразумевает, что система может поглощать возмущения, адаптироваться к новым параметрам и восстанавливаться достаточно быстро, чтобы смягчить последствия нарушений [9].

В настоящее время при управлении ЭЭС используются две системы измерений сбора и обработки информации – SCADA (Supervisory Control And Data Acquisition) и WAMS (Wide Area Measurement System). SCADA-системы, предназначенные для поддержки действий диспетчерского персонала при оперативном и противоаварийном управлении ЭЭС, включают в себя: установленные на подстанциях ЭЭС удаленные устройства телемеханики RTU для снятия телесигналов о состоянии коммутационного оборудования и телеизмерений параметров режима, каналы связи; базы данных; системы оперативного отображения параметров режима, а также программное обеспечение для обработки результатов телеизмерений и формирования управляющих команд для объектов диспетчерского управления. WAMS – широкомасштабная система измерений (Российский аналог СМПР – система мониторинга переходных режимов), предназначенная для проведения мониторинга и управления

1 Работа выполнена в рамках научного проекта «Теоретические основы, модели и методы управления развитием и функционированием интеллектуальных электроэнергетических систем», № FWEU-2021-0001.

2 Колосок Ирина Николаевна, доктор технических наук, ведущий научный сотрудник Лаборатории управления функционированием электроэнергетических систем Института систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, Россия. E-mail: kolosok@isem.irk.ru

3 Гурина Людмила Александровна, кандидат технических наук, доцент, старший научный сотрудник Лаборатории управления функционированием электроэнергетических систем Института систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, Россия. E-mail: gurina@isem.irk.ru

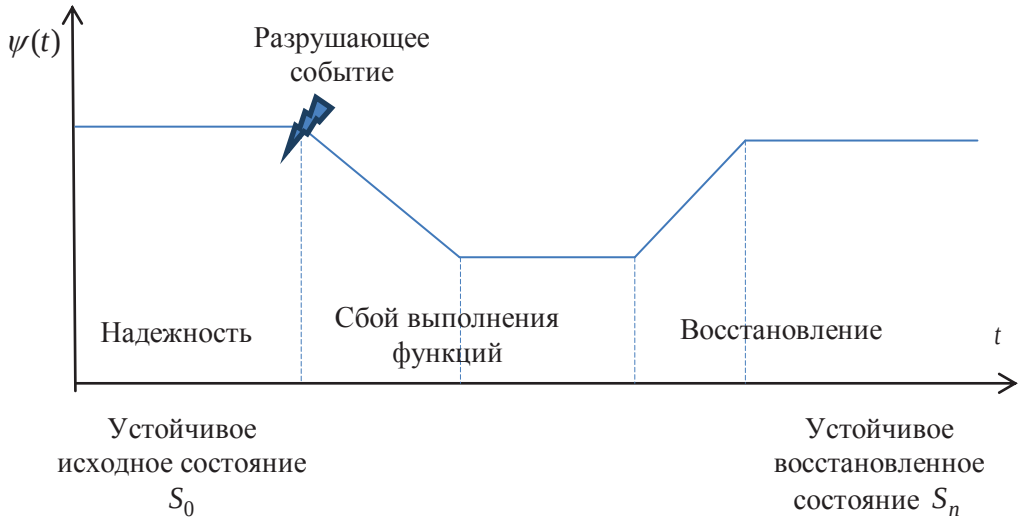

Рис. 1. Переходы между состояниями для описания киберустойчивости SCADA и WAMS

в реальном времени динамическими состояниями ЭЭС и повышения уровня безопасности системы. Система WAMS представляет собой совокупность измерительных устройств PMU, концентраторов векторных данных PDC, каналов передачи информации между PMU, PDC и диспетчерскими центрами, а также средств обработки полученной информации [10, 11].

Системы SCADA и WAMS должны быть киберустойчивыми к экстремальным событиям, в том числе и к кибератакам [12, 13], сохраняя при этом приемлемую функциональность при любых условиях.

Киберустойчивость SCADA и WAMS

Для повышения эффективности управления и обеспечения надежного функционирования ЭЭС были внедрены системы SCADA и WAMS на базе датчиков измерений, средств и технологий передачи и обработки информации на основе разнообразного аппаратного и программного обеспечения, что привело к изменению свойств ЭЭС и созданию киберфизической ЭЭС. Интеграция этих новых технологий привела к большему количеству взаимосвязей и взаимозависимостей между физической и информационно-коммуникационной подсистемами.

Киберустойчивость – это многомерное свойство систем SCADA и WAMS. Сохранение этих свойств требует управления нарушениями, возникающими из-за отказов физических компонентов систем сбора, обработки и передачи информации, кибератак и сбоев процессов, протекающих в информационно-коммуникационной инфраструктуре.

В [14] устойчивость системы определяется как сумма пассивной живучести (надежности) и проактивной живучести (восстановления) системы. Инженерная устойчивость описывается как внутренняя способность системы корректировать свою функциональность при наличии нарушения и непредвиденных изменений.

Таким образом, важные параметры устойчивости (рис. 1.) включают:

1) Надежность, или способность системы поддерживать обычную работу до сбоя;

2) Способность системы предотвращать отрицательные воздействия после разрушающего события;

3) Возможность восстановления, или способность системы своевременно восстанавливаться после разрушающего события.

Показатель киберустойчивости может быть представлен как сумма показателей пассивной живучести (надежности) R и проактивной живучести (восстановления) ρ после нарушения представляется как:

$$\Psi(resilience) = R(reliability) + \rho(restoration), \quad (1)$$

где R — вероятность безотказной работы,
ρ — вероятность восстановления системы.

Показатель киберустойчивости может принимать значения на интервале [0,1]. Ψ равно 0, когда операция восстановления не выполняется, и принимает значение 1, когда система полностью восстанавливается.

Киберустойчивость информационно-коммуникационной инфраструктуры может быть обеспечена за счет уменьшения уязвимостей системы или увеличения скорости восстановления системы.

Благодаря включению надежности показатель киберустойчивости можно более эффективно рассчитать с помощью методов исследования отказов.

Анализ надежности систем сбора и обработки информации для оценки киберустойчивости на примере системы WAMS

СМПР или WAMS базируются на синхронизированных векторных измерениях параметров электрического режима (СВИ). СВИ – совокупность векторных и скалярных параметров режима ЭЭС, измеренных и рассчитанных с заданной дискретизацией в однозначно определенные моменты времени, синхронизиро-

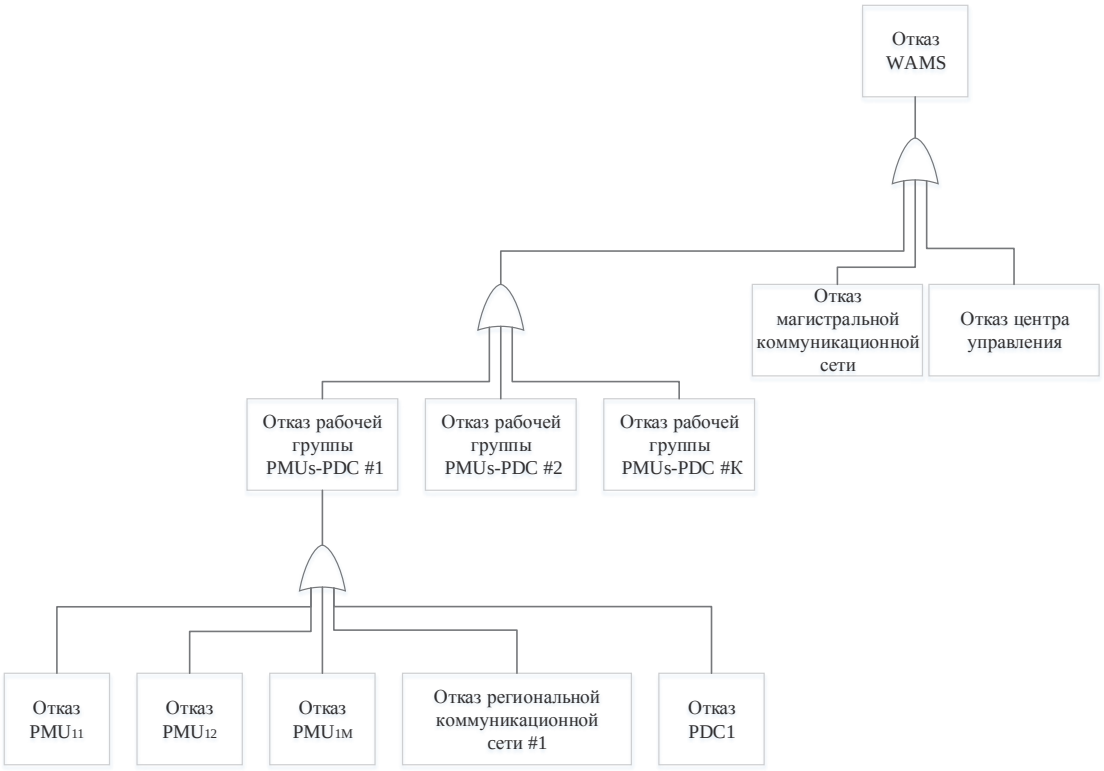

Рис. 2. Дерево отказов WAMS

ванные с помощью глобальных навигационных спутниковых систем [15].

Любые сбои, даже в небольшой части WAMS, могут привести к потере наблюдаемости расчетной схемы ЭЭС. [16]. Надежность функционирования WAMS определяется надежностью каждого из ее элементов.

Анализ пассивной живучести такой иерархической структуры, как WAMS может быть проведен с использованием методов анализа дерева отказов [17, 18] (рис. 2).

Оценка надежности WAMS потребует анализа безотказной работы ее компонентов, например, PMU.

PMU — это цифровой регистратор данных с дополнительной функцией синхронизации.

PMU используют программные алгоритмы для выполнения определенных функций, таких как вычисление амплитуды и угла векторов, вычисление симметричной составляющей, оценка частоты и изменение частоты, определение содержания гармоник и т. д. Очевидно, что программное обеспечение может содержать программные ошибки и поэтому работать неправильно в некоторых ситуациях. Такие аномалии могут вызывать отказы PMU, которые необходимо соответствующим образом моделировать при оценке надежности.

Отказы PMU могут возникать и из-за отказов аппаратного обеспечения. Большинство критически важных для безопасности модемных систем, таких как PMU, характеризуются непосредственной близостью аппаратных и программных операций, что приводит к коррелированным сбоям. Это называется отказом аппаратно-программного взаимодействия [19]. Ошибки программного обеспечения могут привести к сбоям PMU.

При анализе киберустойчивости WAMS предлагается усовершенствованная модель надежности PMU, которая учитывает влияние отказов аппаратного обеспечения, отказов программного обеспечения, отказов аппаратно-программного взаимодействия, представленная на рис. 3.

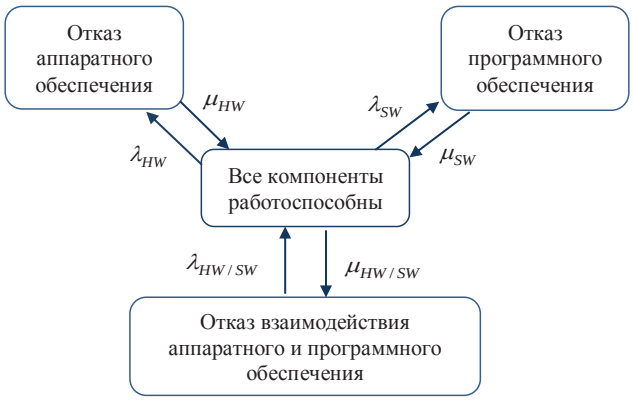

Рис. 3. Модель надежности PMU[4]

Тогда надежность PMU может быть определена как

$$R_{PMU} = R_{HW} R_{SW} R_{HW/SW},$$

4 На рис.3 показаны интенсивность отказа λ и интенсивность восстановления μ для каждого компонента PMU и их взаимодействия

Рис. 4. Надежность сети WAMS

где R_{HW} — надежность аппаратного обеспечения, R_{SW} — надежность программного обеспечения, $R_{HW/SW}$ — надежность взаимодействия аппаратного и программного обеспечения.

PDC, в основном, состоит из компонентов двух типов — программных и аппаратных. Отказ любого компонента может привести к отказу всего устройства. Поэтому надежность PDC определяется аналогично определению надежности PDC.

Еще одной составляющей надежности WAMS является надежность сети [20], причины нарушения которой представлены на рис. 4.

Отказ программного обеспечения (ПО) связан с его несоответствием поставленным задачам. Надежность ПО – есть вероятность того, что программа какой-то период времени будет работать без сбоев с учетом степени их влияния на выходные результаты. ПО не подвержено износу и его надежность определяется только ошибками разработки.

Нарушение киберустойчивости WAMS может быть вызвано и успешно проведенными кибератаками [21-26] на любой из компонентов системы. В табл. 1. приведены примеры кибератак, успешная реализация которых влияет на качество информации [27], используемой при управлении ЭЭС.

Рассмотренные возможные отказы WAMS и причины их возникновения необходимо учитывать и при разработке и выборе мер по обеспечению возможности восстановления системы при нарушении ее функционирования.

Так, при оценке киберустойчивости систем измерений, передачи и обработки информации необходим анализ возможных сбоев, нарушающих качество информации (доступность, целостность, конфиденциальность), требуемой для управления ЭЭС.

Таблица 1

Кибератаки на WAMS, влияющие на качество измерений, используемых при управлении ЭЭС

Угрозы	WAMS	Последствия для качества измерений
FDI-атаки	PMU, PDC, управляющий центр	достоверность
TSA-атаки (spoofing-атаки и др.)	GPS, каналы передачи	достоверность, синхронизация измерений
DoS- , jamming-атаки	Каналы передачи	доступность, своевременность
Атаки повторного воспроизведения, DDoS-атаки	Каналы передачи	достоверность, доступность
Скоординированные атаки	Любой из компонентов WAMS	достоверность, доступность
Вредоносное ПО (Backdoor, Virus, worms, Trojan hors)	Любой из компонентов WAMS	достоверность, доступность, согласованность измерений, конфиденциальность
Атака «человек посередине»	Каналы передачи	достоверность, доступность, конфиденциальность

DOI:10.21681/2311-3456-2021-6-2-11

Таблица 2

Описание состояний системы

Состояние	Описание
N	Нормальное состояние
DE	Разрушающее событие
D	Состояние обнаружения разрушающего события при оценивании состояния
FP	Состояние защиты функций при разрушающем событии
UD	Состояние необнаружения разрушающего события
SD	Состояние медленной деградации
F	Состояние отказа

Например, доступность СВИ, требуемых для мониторинга ЭЭС в установившемся режиме, отслеживания динамического поведения системы, принятия своевременных решений по управлению системой и проверки моделей ЭЭС, может быть нарушена, когда:
– система PMU не может сформировать синхронизированные измерения: либо измерения напряжения и тока, либо спутниковые сигналы GPS.
– система PMU не может доставить данные измерений на верхний уровень управления (PDC или центр управления). Для приложений, работающих в режиме, близком к реальному времени, сеть СВИ должна очень быстро передавать, принимать и упорядочивать данные через несколько уровней PDC и каналы связи между точкой измерения и центром управления.

Оценку показателей киберустойчивости WAMS предлагается проводить на основе моделей полумарковских процессов (ПМП). Основным преимуществом предлагаемого подхода является возможность учета мер по восстановлению системы при разрушающих событиях в моделях полумарковских процессов, то есть показателя ρ модели киберустойчивости (1).

Алгоритм определения показателя киберустойчивости WAMS

При разработке алгоритма рассмотрен случай определения показателя киберустойчивости WAMS с учетом доступности СВИ, используемых при выработке управляющих воздействий на технологическую часть киберфизической ЭЭС. По аналогии на основе предложенного алгоритма можно определить показатели киберустойчивости при нарушении целостности и конфиденциальности данных. Тогда показатель (вероятность) киберустойчивости WAMS, учитывающий качество измерений можно представить как

$$\Psi = \Psi_A \Psi_I \Psi_C , \qquad (2)$$

где Ψ_A — показатель киберустойчивости при нарушении доступности измерений, Ψ_I — показатель киберустойчивости при нарушении целостности измерений, Ψ_C — показатель киберустойчивости при нарушении конфиденциальности измерений.

При оценке киберустойчивости при нарушении доступности измерений PMU диаграмму переходов состояний (табл. 2) полумарковской модели системы WAMS с учетом мер по восстановлению системы (оценивание состояний, защита функционирования при разрушающих событиях) можно представить, как показано на рис. 5. Модель ПМП основана на случайном процессе {X(t): t≥0} с дискретным пространством состояний $X_S\{N, DE, D, FP, UD, SD, F\}$. Эта обобщенная модель позволяет использовать несколько стратегий сохранения киберустойчивости при различных разрушающих событиях.

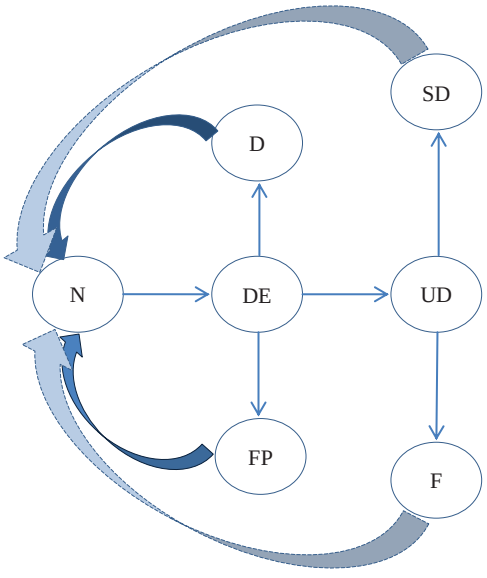

Рис. 5. Диаграмма переходов состояний системы на основе полумарковских процессов с учетом мер по обеспечению доступности

Киберустойчивая система может находиться в состояниях $\{N, FP, D\}$ и, при принятии мер по устранению

последствий разрушающего события, возвращается в состояние N. Если устойчивость системы нарушается, то система переходит в состояния $\{SD, F\}$. Обнаружение и смягчение последствий разрушающего события для качества информации методами ОС снижает вероятность перехода системы в пространство состояний $\{SD, F\}$ и создает возможность возврата системы в состояние $\{N\}$.

Основу обеспечения киберустойчивости при наличии разрушающих событий составляют следующие меры — обнаружение ошибок, оценка повреждений, восстановление после ошибок и обработка ошибок.

Важную роль для обнаружения ошибок, смягчения последствий и подавления их влияния для того, чтобы WAMS находилась или возвращалась в устойчивое состояние, играют методы оценивания состояния (ОС) ЭЭС.

ОС ЭЭС включает в себя выполнение таких функций как анализ наблюдаемости ЭЭС, обработка конфигурации сети (анализ топологии сети), идентификация «плохих данных», фильтрация погрешностей измерений, дорасчет неизмеренных параметров.

Таким образом, обнаружение и смягчение последствий разрушающего события для качества информации методами ОС [28, 29] снижает вероятность перехода системы в пространство состояний $\{SD, F\}$ и создает возможность перехода системы в состояние $\{N\}$.

В качестве мер обеспечения возможности перехода системы в состояние $\{FP\}$ и, в дальнейшем, возвращалась в состояние $\{N\}$, могут служить оптимальная расстановка PMU [30, 31] для сохранения наблюдаемости, дублирование каналов связи и др.

Показатель киберустойчивости описывается согласно (1). Нарушение доступности может вызвать переход WAMS в состояние медленной деградации SD или в состояние отказа F. Отсюда, показатель киберустойчивости системы, описываемый моделью (1), при нарушении доступности можно определить исходя из следующего выражения

$$\Psi_A = 1 - (\pi_{SD} + \pi_F), \qquad (3)$$

где π_{SD}, π_F — установившиеся (стационарные) вероятности состояний SD и F соответственно, то есть когда доступность измерений нарушена.

Показатель киберустойчивости определяется согласно следующему алгоритму:

1. *Определение матрицы вероятностей перехода*

При заданных интервалах времени нахождения системы в различных состояниях $[a, b]$ определяются вероятности перехода:

$$P(Y < X) = \int_a^b \frac{t}{b}\frac{1}{b-a}dt \ , \ P_N = \lim_{t\to\infty} F_N(t) = 1 \ ,$$

$$P_F = \lim_{t\to\infty} F_F(t) = 1 \ ,$$

и составляется матрица вероятностей перехода

$$P = \begin{array}{c} \\ N \\ D \\ FP \\ SD \\ F \end{array} \begin{array}{c} \begin{array}{ccccc} N & D & FP & SD & F \end{array} \\ \begin{pmatrix} 0 & p_N & 0 & 0 & 0 \\ p_D & 0 & 1-p_D & 0 & 0 \\ p_{FP} & 0 & 0 & 1-p_{FP} & 0 \\ p_{SD} & 0 & 0 & 0 & 1-p_{SD} \\ 0 & 0 & 0 & 0 & p_F \end{pmatrix} \end{array},$$

$$\sum_{j=1}^{n} p_{ij} = 1, \forall i = \overline{1,n}.$$

Матрицу P можно представить как

$$P = \begin{pmatrix} Q & C \\ 0 & E \end{pmatrix},$$

где Q – фундаментальная матрица, элементами которой являются вероятности перехода между переходными состояниями, C – матрица вероятностей перехода между переходными и поглощающими состояниями, E – единичная матрица.

2. *Определение среднего времени пребывания в состоянии i*

Среднее время пребывания S_i определяется согласно выражению

$$S_i = \int_0^{a_i}(1-\frac{t}{b_i})dt + \int_{a_i}^{b_i}(1-\frac{t}{b_i})(1-\frac{t-a_i}{b_i-a_i})dt \ ,$$

3. *Определение среднего времени до отказа*

$$MTTF = \sum_{i\in Trans} M_i S_i \ ,$$

где M_i — количество посещений переходного состояния i до того, как модель перейдет в поглощающее состояние, S_i — среднее время пребывания в состоянии i. Для нахождения M_i определяется матрица M

$$M = [m_{ij}] = (E-Q)^{-1} \ ,$$

где m_{ij} — среднее количество посещения состояния j перед переходом в поглощающее состояние, учитывая, что модель запущена в состоянии i.

4. *Определение стационарных распределений вероятностей состояний марковской цепи*

Поскольку у нас 5 состояний, вектор V, элементами которого являются стационарные распределения вероятностей вложенной марковской цепи, запишем следующим образом:

$$V = [v_N, v_D, v_{FP}, v_{SD}, v_F] \ .$$

Причем,

$$v_N + v_D + v_{FP} + v_{SD} + v_F = 1 \ .$$

Делая поглощающее состояние F переходным и в соответствии с этим преобразовав матрицу P, определяется вектор V.

5. *Определение установившихся вероятностей состояний системы*

Установившиеся вероятности определяются согласно следующего выражения

$$\pi_i = \frac{v_i s_i}{\sum_{i=1}^{n} v_i s_i}.$$

6. Определение показателя киберустойчивости системы

По формуле (3) определяется показатель киберустойчивости ψ_A при нарушении доступности измерений.

Пример

Пусть интервалы времени пребывания (час.) системы в каждом из состояний следующие: $T_N = [70, 350]$; $T_D = [20, 550]$; $T_{FP} = [5, 300]$; $T_{SD} = [5, 50]$; $T_F = [1, 350]$.

1. Определяем вероятности перехода и составляем матрицу вероятностей перехода

$$P = \begin{array}{c} \begin{matrix} N & D & FP & SD & F \end{matrix} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0.52 & 0 & 0.48 & 0 & 0 \\ 0.51 & 0 & 0 & 0.49 & 0 \\ 0.55 & 0 & 0 & 0 & 0.45 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array},$$

2. Среднее время пребывания (час.) в состоянии i

$S_N = 210$, $S_{SE} = 190$, $S_{FP} = 101.66$,$S_{SD} = 18.26$, $S_F = 25.5$.

3. Среднее время до отказа

$MTTF = 4280.82$ час.

4. Стационарные вероятности вложенной марковской цепи

$v_N = 0.354$, $v_D = 0.354$, $v_{FP} = 0.17$, $v_{SD} = 0.083$, $v_F = 0.037$.

5. Установившиеся вероятности

$\pi_N = 0.46$, $\pi_D = 0.417$, $\pi_{FP} = 0.107$, $\pi_{SD} = 0.009$, $\pi_F = 0.006$.

6. Показатель киберустойчивости при нарушении доступности с учетом мер по восстановлению $\psi_A = 0.985$.

Выводы

1. Проведен анализ причин нарушения киберустойчивости систем сбора и обработки информации, требуемой при управлении ЭЭС. Показано влияние нарушения безотказной работы компонентов на киберустойчивость всей системы сбора и обработки информации на примере WAMS.

2. Предложена модель надежности PMU, составляющие которой влияют на киберустойчивость WAMS.

3. Предложена модель WAMS на основе полумарковских процессов, позволяющая учитывать возможные состояния системы при нормальном функционировании и при нарушении ее киберустойчивости.

4. Разработан алгоритм определения показателя киберустойчивости WAMS, учитывающий меры по восстановлению системы при нарушении качества синхронизированных векторных измерений.

Достоверность исследования подтверждается:

– наличием и учетом нормативных документов по применению методов анализа надежности, марковских методов в технических системах;

– строгим соответствием определениям устойчивости инженерных систем при разработке алгоритма определения показателей киберустойчивости.

Литература

1. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. In IEEE Access. 2020, vol. 8, pp. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826
2. X. Chu, M. Tang, H. Huang and L. Zhang. A security assessment scheme for interdependent cyber-physical power systems. 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2017, pp. 816-819, DOI: 10.1109/ICSESS.2017.8343036
3. Воропай Н.И. Направления и проблемы трансформации электроэнергетических систем // Электричество. 2020. № 7. С. 12-21. DOI: 10.24160/0013-5380-2020-7-12-21
4. M. Ni and M. Li. Reliability Assessment of Cyber Physical Power System Considering Communication Failure in Monitoring Function. 2018 International Conference on Power System Technology (POWERCON). 2018, pp. 3010-3015. DOI: 10.1109/POWERCON.2018.8601964
5. Jia Guo, Yifei Wang, Chuangxin Guo, Shufeng Dong and Baijian Wen. Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741899
6. Колосок И.Н., Гурина Л.А. Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств // Методические вопросы исследования надежности больших систем энергетики. В 2-х книгах. 2019. С. 238-247.
7. S. Sridhar, A. Ashok, M. Mylrea, S. Pal, M. Rice and S. N. G. Gourisetti. A testbed environment for buildings-to-grid cyber resilience research and development. 2017 Resilience Week (RWS). 2017, pp. 12-17. DOI: 10.1109/RWEEK.2017.8088641
8. Воропай Н.И., Колосок И.Н., Коркина Е.С. Проблемы повышения киберустойчивости цифровой подстанции // Релейная защита и автоматизация. 2019. № 1(34). С. 78-83.

9. Voropai N Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, vol.13. No.21. DOI: 10.3390/en13215639
10. Kolosok I.N., Gurina, L. A. (2017). Determination of the vulnerability index to cyberattacks and state-estimation problems according to SCADA data and timed vector measurements. Russian Electrical Engineering. 2017, vol. 88(1), pp. 23–29. DOI:10.3103/s1068371217010096
11. X. Liu, X. Zeng, L. Yao, G. I. Rashed and C. Deng. Power System State Estimation Based on Fusion of WAMS/SCADA Measurements: A Survey. 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2). 2018, pp. 1-6. DOI: 10.1109/EI2.2018.8582102.
12. I. Kolosok and L. Gurina. Wavelet Analysis of PMU Measurements for Identification of Cyber Attacks on TCMS. 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2018, pp. 1-4. DOI: 10.1109/ICIEAM.2018.8728768
13. R. Kateb, P. Akaber, M. H. K. Tushar, A. Albarakati, M. Debbabi and C. Assi. Enhancing WAMS Communication Network Against Delay Attacks. In IEEE Transactions on Smart Grid. May 2019, vol. 10, no. 3, pp. 2738-2751. DOI: 10.1109/TSG.2018.2809958
14. Seyedmohsen Hosseini, Kash Barker, Jose E. Ramirez-Marquez. A review of definitions and measures of system resilience. Reliability Engineering & System Safety. 2016, vol. 145, p. 47-61. DOI:10.1016/j.ress.2015.08.006
15. Жуков А.В., Сацук Е.И., Дубинин Д.М., Опалев О.Л., Уткин Д.Н. Вопросы применения технологии синхронизированных векторных измерений для задач мониторинга эксплуатационного состояния электрооборудования // Энергетик. 2017. №9. С. 3-8.
16. Голуб И.И., Хохлов М.В. Алгоритмы синтеза наблюдаемости ЭЭС на основе синхронизированных векторных измерений // Электричество. 2015. №1. С.26-33.
17. Ankur Singh Rana, Mini S. Thomas, Nilanjan Senroy. Reliability evaluation of WAMS using Markov-based graph theory approach. Generation Transmission & Distribution IET. 2017, vol. 11, no. 11, pp. 2930-2937. DOI: 10.1049/iet-gtd.2016.0848
18. C. Murthy, D. S. Roy and D. K. Mohanta. Re-estimation of hidden Markov model parameters of Phasor Measurement Unit. 2015 IEEE Power, Communication and Information Technology Conference (PCITC). 2015, pp. 379-384. DOI: 10.1109/PCITC.2015.7438195
19. Diptendu Sinha Roy, Cherukuri Murthy, Dusmanta Kumar Mohanta. Reliability analysis of phasor measurement unit incorporating hardware and software interaction failures. Generation Transmission & Distribution IET. 2015, vol. 9, no. 2, pp. 164-171. DOI: 10.1049/iet-gtd.2014.0115
20. Успенский М.И. Составляющие надежности информационной сети системы мониторинга переходных режимов // Методические вопросы исследования надежности больших систем энергетики. 2020. С. 370-379.
21. 21. A. Ashok, M. Govindarasu and J. Wang. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. In Proceedings of the IEEE. July 2017, vol. 105, no. 7, pp. 1389-1407. DOI: 10.1109/JPROC.2017.2686394
22. A. Ashok, M. Govindarasu and V. Ajjarapu. Attack-resilient measurement design methodology for State Estimation to increase robustness against cyber attacks. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741979
23. P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore and R. S. Blum. GPS spoofing attack characterization and detection in smart grids. 2016 IEEE Conference on Communications and Network Security (CNS). 2016, pp. 391-395. DOI: 10.1109/CNS.2016.7860525
24. A. Huseinović, S. Mrdović, K. Bicakci and S. Uludag. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. In IEEE Access. 2020, vol. 8, pp. 177447-177470. DOI: 10.1109/ACCESS.2020.3026923
25. J. Yan, Y. Tang, Bo Tang, H. He and Y. Sun. Power grid resilience against false data injection attacks. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741850
26. G. Coletta, A. Pepiciello, A. Vaccaro, D. Villacci and G. M. Giannuzzi. Time Synchronization Attack in Synchrophasors-based Dynamic Thermal Rating Assessment: Impact and Analysis. 2018 AEIT International Annual Conference. 2018, pp. 1-6. DOI: 10.23919/AEIT.2018.8577398.
27. Колосок И.Н., Гурина Л.А. Оценка качества данных SCADA и WAMS при кибератаках на информационно-коммуникационную инфраструктуру ЭЭС // Информационные и математические технологии в науке и управлении. 2020. № 1(17). С. 68-78. DOI: 10.38028/ESI.2020.17.1.005
28. 28. Колосок И.Н., Гурина Л.А. Идентификация кибератак на системы SCADA и СМПР в ЭЭС при обработке измерений методами оценивания состояния // Электричество. 2021. № 6. С. 25–32. DOI: 10.24160/0013-5380-2021-6-25-32
29. Колосок И.Н., Гурина Л.А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. 2018. № 3(27). С. 63–69. DOI: 10.21681/2311-3456-2018-3-63-69
30. M. V. Khokhlov, O. A. Pozdnyakova and A. Obushevs. Optimal PMU Placement for Power System State Estimation using Population-based Algorithms Incorporating Observability Requirements. 2020 IEEE 61st International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON). 2020, pp. 1-8. DOI: 10.1109/RTUCON51174.2020.9316476
31. Y. Yao, X. Liu and Z. Li. Robust Measurement Placement for Distribution System State Estimation. In IEEE Transactions on Sustainable Energy. Jan. 2019, vol. 10, no. 1, pp. 364-374. DOI: 10.1109/TSTE.2017.2775862

ASSESSMENT OF CYBER RESILIENCE INDICES OF INFORMATION COLLECTION AND PROCESSING SYSTEMS IN ELECTRIC POWER SYSTEMS BASED ON SEMI-MARKOV MODELS[5]

Kolosok I.N. [6], Gurina L.A.[7]

Purpose of the study: *The study aims to design an algorithm for determining the cyber resilience indices of information collection, transmission, and processing systems (SCADA, WAMS) to control electric power systems. This algorithm makes it possible to factor in possible states and measures to restore such systems when cyber resilience is lost.*

Research methods *include the probability theory, methods of power system reliability analysis, and Markov methods.*

Result of the research: *The analysis of the reliability of WAMS, which is necessary for assessing the cyber resilience of the EPS, has been carried out. A cyber resilience model is proposed, on the basis of which an algorithm for determining the cyber resilience index of SCADA, WAMS systems with a low quality of measurement information used in EPS control has been developed. To take into account possible states of SCADA, WAMS systems and measures for their restoration (detection, mitigation and response) in case of violation of cyber resilience, the algorithm uses the tools of probability theory and Markov methods. The effectiveness of the application of the developed algorithm is confirmed by the example of calculating the WAMS cyber resilience index with a low quality of PMU data. The results obtained can be useful in making decisions on the formation of control actions on the EPS to ensure its cybersecurity in the context of cyber-attacks on information collection, transmission, and processing systems.*

Keywords: *electric power system, reliability, resilience, SCADA, WAMS, cyber-attacks, measurement quality, state estimation.*

References

1. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. In IEEE Access. 2020, vol. 8, pp. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826
2. X. Chu, M. Tang, H. Huang and L. Zhang. A security assessment scheme for interdependent cyber-physical power systems. 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2017, pp. 816-819, DOI: 10.1109/ICSESS.2017.8343036
3. Воропай Н.И. Napravleniya i problemy transformacii elektroenergeticheskih sistem, Elektrichestvo [Elektrichestvo], 2020, № 7, pp. 12-21. DOI: 10.24160/0013-5380-2020-7-12-21
4. M. Ni and M. Li. Reliability Assessment of Cyber Physical Power System Considering Communication Failure in Monitoring Function. 2018 International Conference on Power System Technology (POWERCON). 2018, pp. 3010-3015. DOI: 10.1109/POWERCON.2018.8601964
5. Jia Guo, Yifei Wang, Chuangxin Guo, Shufeng Dong and Baijian Wen. Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741899
6. Kolosok I.N., Gurina L.A. Ocenka riskov upravleniya kiberfizicheskoj EES na osnove teorii nechetkih mnozhestv // Metodicheskie voprosy issledovaniya nadezhnosti bol'shih sistem energetiki [Methodological problems reliability study of large energy systems], v 2-h knigah, 2019, pp. 238-247.
7. S. Sridhar, A. Ashok, M. Mylrea, S. Pal, M. Rice and S. N. G. Gourisetti. A testbed environment for buildings-to-grid cyber resilience research and development. 2017 Resilience Week (RWS). 2017, pp. 12-17. DOI: 10.1109/RWEEK.2017.8088641
8. Voropaj N.I., Kolosok I.N., Korkina E.S. Problemy povysheniya kiberustojchivosti cifrovoj podstancii // Relejnaya zashchita i avtomatizaciya [Relay protection and automation], 2019, № 1(34), pp. 78-83.
9. Voropai N Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, vol.13. No.21. DOI: 10.3390/en13215639

5 The research was conducted within the framework of the scientific project «Theoretical foundations, models and methods to control the expansion and operation of intelligent electric power systems (Smart Grids)», No. FWEU-2021-0001.

6 Irina N. Kolosok, Dr.Sc. in engineering, Lead Researcher in the Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: kolosok@isem.irk.ru

7 Liudmila A. Gurina, Ph.D. in engineering, Associate Professor, Senior Researcher in the Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E mail: gurina@isem.irk.ru

10. Kolosok I.N., Gurina, L. A. (2017). Determination of the vulnerability index to cyberattacks and state-estimation problems according to SCADA data and timed vector measurements. Russian Electrical Engineering. 2017, vol. 88(1), pp. 23–29. DOI:10.3103/s1068371217010096
11. X. Liu, X. Zeng, L. Yao, G. I. Rashed and C. Deng. Power System State Estimation Based on Fusion of WAMS/SCADA Measurements: A Survey. 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2). 2018, pp. 1-6, DOI: 10.1109/EI2.2018.8582102.
12. I. Kolosok and L. Gurina. Wavelet Analysis of PMU Measurements for Identification of Cyber Attacks on TCMS. 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2018, pp. 1-4. DOI: 10.1109/ICIEAM.2018.8728768
13. R. Kateb, P. Akaber, M. H. K. Tushar, A. Albarakati, M. Debbabi and C. Assi. Enhancing WAMS Communication Network Against Delay Attacks. In IEEE Transactions on Smart Grid. May 2019, vol. 10, no. 3, pp. 2738-2751. DOI: 10.1109/TSG.2018.2809958
14. Seyedmohsen Hosseini, Kash Barker, Jose E. Ramirez-Marquez. A review of definitions and measures of system resilience. Reliability Engineering & System Safety. 2016, vol. 145, p. 47-61. DOI: 10.1016/j.ress.2015.08.006
15. Zhukov A.V., Sacuk E.I., Dubinin D.M., Opalev O.L., Utkin D.N. Voprosy primeneniya tekhnologii sinhronizirovannyh vektornyh izmerenij dlya zadach monitoringa ekspluatacionnogo sostoyaniya elektrooborudovaniya, Energetik [Energetick], 2017, № 9, pp. 3-8.
16. Golub I.I., Hohlov M.V. Algoritmy sinteza nablyudaemosti EES na osnove sinhronizirovannyh vektornyh izmerenij, Elektrichestvo [Elektrichestvo], 2015, № 1, pp. 26-33.
17. Ankur Singh Rana, Mini S. Thomas, Nilanjan Senroy. Reliability evaluation of WAMS using Markov-based graph theory approach. Generation Transmission & Distribution IET. 2017, vol. 11, no. 11, pp. 2930-2937. DOI: 10.1049/iet-gtd.2016.0848
18. C. Murthy, D. S. Roy and D. K. Mohanta. Re-estimation of hidden Markov model parameters of Phasor Measurement Unit. 2015 IEEE Power, Communication and Information Technology Conference (PCITC). 2015, pp. 379-384. DOI: 10.1109/PCITC.2015.7438195
19. Diptendu Sinha Roy, Cherukuri Murthy, Dusmanta Kumar Mohanta. Reliability analysis of phasor measurement unit incorporating hardware and software interaction failures. Generation Transmission & Distribution IET. 2015, vol. 9, no. 2, pp. 164-171. DOI: 10.1049/iet-gtd.2014.0115
20. Uspenskij M.I. Sostavlyayushchie nadezhnosti informacionnoj seti sistemy monitoringa perekhodnyh rezhimov // Metodicheskie voprosy issledovaniya nadezhnosti bol'shih sistem energetiki [Methodological problems reliability study of large energy systems], 2020, pp. 370-379.
21. A. Ashok, M. Govindarasu and J. Wang. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. In Proceedings of the IEEE. July 2017, vol. 105, no. 7, pp. 1389-1407. DOI: 10.1109/JPROC.2017.2686394
22. A. Ashok, M. Govindarasu and V. Ajjarapu. Attack-resilient measurement design methodology for State Estimation to increase robustness against cyber-attacks. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp. 1-5. DOI: 10.1109/PESGM.2016.7741979
23. P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore and R. S. Blum. GPS spoofing attack characterization and detection in smart grids. 2016 IEEE Conference on Communications and Network Security (CNS). 2016, pp. 391-395. DOI: 10.1109/CNS.2016.7860525
24. A. Huseinović, S. Mrdović, K. Bicakci and S. Uludag. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. In IEEE Access. 2020, vol. 8, pp. 177447-177470. DOI: 10.1109/ACCESS.2020.3026923
25. J. Yan, Y. Tang, Bo Tang, H. He and Y. Sun. Power grid resilience against false data injection attacks. 2016 IEEE Power and Energy Society General Meeting (PESGM). 2016, pp.1 5. DOI: 10.1109/PESGM.2016.7741850
26. G. Coletta, A. Pepiciello, A. Vaccaro, D. Villacci and G. M. Giannuzzi. Time Synchronization Attack in Synchrophasors-based Dynamic Thermal Rating Assessment: Impact and Analysis. 2018 AEIT International Annual Conference. 2018, pp. 1-6. DOI: 10.23919/AEIT.2018.8577398
27. Kolosok I.N., Gurina L.A. Ocenka kachestva dannyh SCADA i WAMS pri kiberatakah na informacionno-kommunikacionnuyu infrastrukturu EES // Informacionnye i matematicheskie tekhnologii v nauke i upravlenii [Information and mathematical tehnologies in science and management], 2020, № 1(17), pp. 68-78. DOI: 10.38028/ESI.2020.17.1.005
28. Kolosok I.N., Gurina L.A. Identifikaciya kiberatak na sistemy SCADA i SMPR v EES pri obrabotke izmerenij metodami ocenivaniya sostoyaniya // Elektrichestvo [Elektrichestvo], 2021, № 6, pp. 25-32. DOI: 10.24160/0013-5380-2021-6-25-32
29. Kolosok I.N., Gurina L.A. Povyshenie kiberbezopasnosti intellektual'nyh energeticheskih sistem metodami ocenivaniya sostoyaniya // Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, № 3(27), pp. 63-69. DOI: 10.21681/2311-3456-2018-3-63-69
30. M. V. Khokhlov, O. A. Pozdnyakova and A. Obushevs. Optimal PMU Placement for Power System State Estimation using Population-based Algorithms Incorporating Observability Requirements. 2020 IEEE 61th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON). 2020, pp. 1-8. DOI: 10.1109/RTUCON51174.2020.9316476
31. Y. Yao, X. Liu and Z. Li. Robust Measurement Placement for Distribution System State Estimation. In IEEE Transactions on Sustainable Energy. Jan. 2019, vol. 10, no. 1, pp. 364-374. DOI: 10.1109/TSTE.2017.2775862